

REMARKS

Applicant submits this Reply in response to the non-final Office Action mailed October 24, 2008. Before this Reply, claims 42-82 were pending, of which claims 42, 69, and 77 were independent. In the Office Action, the Examiner rejected claim 42 under 35 U.S.C. § 112, ¶ 1, for failing to comply with the enablement requirement.¹ The Examiner rejected each of the claims 42-82 under 35 U.S.C. § 103(a) as being unpatentable over Viktor Fischer et al., *Two Methods of Rijndael Implementation in Reconfigurable Hardware*, 2162 Lecture Notes in Computer Science, Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems 77 (May 14-16 2001) ("Viktor") in view of U.S. Patent No. 5,261,003 ("Matsui"). In this response, Applicant has amended claims 42, 69, and 77. Support for these amendments can be found in the specification at, for example, p. 7, ll. 5-15 and Fig. 1. No new matter has been added. Applicant has also amended portions of the specification to correct minor typographical errors therein. Accordingly, claims 42-82 are currently pending, of which claims 42, 69, and 77 independent. Applicant respectfully traverses all pending rejections and requests reconsideration of the application, as amended.

Rejection Under 35 U.S.C. § 112, ¶ 1

Applicant traverses the rejection of claim 42 under 35 U.S.C. § 112, ¶ 1 for failing to comply with the enablement requirement. The Office Action alleges that "[t]he

¹ The Office Action contains a number of statements reflecting characterizations of the Applicant's disclosure, including the claims, and the related art. Regardless of whether any such statement is specifically addressed herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

claim(s) contain subject matter which was not described in the specification in such a way as to enable one skilled in the art . . . to make and/or use the invention.” Office Action, p. 2. More specifically, the Office Action appears to allege that the recitation of “selecting k out of $2^m k$ key bits” does not meet the enablement requirement of 35 U.S.C. § 112, ¶ 1. However, this is not correct.

Applicant submits that the original filed disclosure sufficiently enables one of ordinary skill to practice this feature. For example, the original disclosure provides:

The m control bits 14, which are taken intact to the output 19, are used to select k out of $2^m k$ secret key bits by a multiplexer circuit 4 having m control bits 12, 2^m k -bit inputs, 8, and one k -bit output 10. The multiplexer circuit 4 may be implemented as a $m \times k$ lookup table, i.e., k (binary) $m \times 1$ lookup tables whose content is defined by the secret key.

Specification, at p. 6, l. 32 -p. 7, l. 4. Applicant submits that this passage, along with the balance of the specification, readily enables one of ordinary skill in the art to practice “selecting k out of $2^m k$ key bits.” Indeed, Applicant submits that multiplexer circuits were readily available at the date of the application’s filing, and one of ordinary skill in the art would have been able to implement “selecting k out of $2^m k$ key bits” if provided with Applicant’s disclosure. Accordingly, Applicant respectfully requests that the 35 U.S.C. § 112, ¶ 1 rejection of claim 42 be withdrawn.

Rejections Under 35 U.S.C. § 103(a)

Applicant respectfully traverses the rejection of claims 42-82 under 35 U.S.C. § 103(a) as being unpatentable over Viktor in view of Matsui. The Office Action has not properly resolved the *Graham* factual inquiries, the proper resolution of which is the requirement for establishing a framework for an objective obviousness analysis. See

M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 U.S.P.Q. 459 (1966), as reiterated by the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, 82 U.S.P.Q.2d 1385 (2007).

While Applicant has amended independent claims 42, 69, and 77 to further demonstrate the differences between Matsui and the claims, Applicant maintains that the Office Action has not properly ascertained the differences between the claims and the references, at least because it has not interpreted the references and considered both the claims and the prior art as a whole. See M.P.E.P. § 2141(II)(B).

Representative claim 42, as presently amended, calls for a combination including, for example, “a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits . . . wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input.” Applicant respectfully submits that neither Viktor nor Matsui, either alone or in combination, teaches or suggests at least this element of Applicant's amended independent claim 42.

The Office Action concedes that “Viktor fails to disclose ‘. . . a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits. . . .’” Office Action, p. 4. However, the Office Action contends that Matsui discloses the above-referenced element, and that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Viktor with Matsui to arrive at the subject matter of claim 42. Contrary to the Office Action's contention, Applicant submits that Matsui also fails to teach or suggest “a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits . . .

wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input,” as required by Applicant’s amended independent claim 42.

Matsui generally discloses “a data communication system with a data scrambling.” Matsui, col. 5, ll. 44-45. To that end, Matsui discloses a system in which

[T]he input plaintext 3 is divided into more significant 4 bytes and less significant 4 bytes, and the less significant 4 bytes are input to the processing block 9 and the address calculating circuit 23 through the selector 24. The address calculating circuit 23 calculates and [sic] address of a extended key to be selected on the basis of the input plaintext data and outputs the calculated address to the extended key latch 7. The extended key latch 7 supplies the selected extended key corresponding to the given address to the selector 25, and the key is transmitted to the processing block 9 through the selector 25. The processing block 9 scrambles the input plaintext data by using the selected key of the selector 25 as the parameter and outputs a scrambled data. Then, in the exclusive OR 12, the output data of the processing block 9 and the more significant 4 bytes of the plaintext 3 are calculated, and the calculated result and less significant 4 bytes of the input plaintext data are replaced with each other to output to a next step.

Matsui, col. 6, ll. 4-23.

Matsui fails to disclose or suggest “a transformation circuit, for transforming a remaining portion n of said input block of bits into transformed bits . . . wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input,” as recited in Applicant’s amended independent claim 42. Instead, as noted above, Matsui discloses two steps for scrambling input data before such data is output to the next step. See Matsui, col. 6, ll. 4-23. In the first step, “the less significant 4 bytes are input into the processing block 9,” *id.* at col. 6, ll. 6-7, and “[t]he processing block 9 scrambles the input plain text data by using the selected key.” *Id.* at col. 6, ll. 15-16. Then, in the

second step, “the output data of the processing block 9 and the more significant 4 bytes of the plaintext 3 are calculated, and the calculated result . . . [is] output to a next step.” *Id.* at col. 6, ll. 18-23.

Thus, in order to scramble input data, Matsui’s processing block 9 requires the less significant 4 bytes of the input plain text and selected key as inputs, while exclusive or gate 12 requires the more significant 4 bytes of the input plain text and output of processing block 9, *i.e.*, the 4 less significant bytes of the input plain text scrambled by the selected key, as inputs. In other words, both the less significant 4 bytes and the more significant 4 bytes of the input plain text are required to scramble the input data. Accordingly, Matsui fails to disclose or suggest “a transformation circuit, for transforming a remaining portion *n* of said input block of bits into transformed bits . . . wherein said transformation circuit transforms said remaining portion of said input block of bits without receiving said first portion of said input block of bits as an input,” as recited in Applicant’s amended independent claim 42.

As set forth above Viktor and Matsui do not teach or suggest every feature of Applicant’s amended independent claim 42. Consequently, the Office Action has not properly ascertained the differences between the references and the rejected claim. Accordingly, no reason has been clearly articulated as to why the claim would have been obvious to one of ordinary skill in the art. For at least this reason, claim 42 should be allowable.

Applicant’s amended independent claims 69 and 77, although different in scope from amended independent claim 42, recite similar subject matter and are therefore allowable for at least the same reasons. Dependent claims 43-68, 70-76, and 78-82,

each depend from one of independent claims 42, 69, and 77, and are therefore allowable for at least the same reasons. Applicant therefore respectfully requests that the rejection of claims 42-82 under 35 U.S.C. § 103(a) be withdrawn.

Conclusion

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.


Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: February 20, 2009

By: _____



R. Bruce Bower
Reg. No. 37,099